NIS2 DIRECTIVE

MANAGEMENT CONSULTING | IT CONSULTING | SECURITY CONSULTING

The DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union shall be applicable from 18th of October, 2024 in all member states.

WHO ARE SUBJECTS TO NIS2/ WHO IS IT ABOUT?

According to NIS2, subjects to this directive are

the enterprises and service providers which operate in critical and highly cirtical sectors, also qualify as medium-sized, which means:

- Number of all employees is higher than 50 and
- Annual netto revenue or balance sheet amount is more than 10 million Euros.

Exceptions

Exceptions, where NIS2 is applicable regardless of size:

- providers of public electronic communications networks or of publicly available electronic communications services;
- trust service providers;
- top-level domain name registries
- domain name system service providers.

CRITICAL AND HIGHLY CRITICAL SECTORS

Highly Critical Sectors

- Energy
- Transport
- Banking
- Financial Market Infrastructures
- Health
- Drinking water
- Waste water
- Digital Infrastructure
- ICT Service managements (B2B)
- Public administration

Critical Sectors

- Postal and courier services
- Waste Management
- Manufacture, production and distribution of chemicals
- Production, processing and distribution of food
- Manufacturing
- Digital Providers
- Research

DEADLINES

According to NIS2, all enterprises have to admit their required information to the national registry by 17th January, 2025.

Data must include:

- the name of the entity;
- the relevant sector, subsector and type of entity
- the address of the entity's main establishment and its other legal establishments in the Union
- up-to-date contact details, including email addresses and telephone numbers of the entity and, where applicable, its representative
- the Member States where the entity provides services; and
- the entity's IP ranges.

By 17th October 2024 every member state has to accept and promulgate national legislations.

All further deadlines only concern the member states and their competent national authorities:

By 17 April 2025, Member States shall establish a list of essential and important entities as well as entities providing domain name registration services. Every two years thereafter, the competent authorities shall be notified.

By 17 January 2025, and every two years thereafter, the CSIRTs network shall, for the purpose of the review referred to in Article 40, assess the progress made with regard to the operational cooperation and adopt a report.

AAM CONSULTING

AAM Consulting
Capital Square Offices, 76, Váci út,
1133 Budapest, Hungary
Phone: +36 1 465 2070, +36 1 688 66 88
Web: https://www.aam.hu/
E-mail: aam@aam.hu

AAM Consulting Bulgaria
17, ul. Moskovska,
1000 Sofia, Bulgaria
Phone: +359 878 32 03 04
Web: https://www.aamconsulting.bg/
E-mail: aambulgaria@aam.hu

NIS2 DIRECTIVE

MANAGEMENT CONSULTING | IT CONSULTING | SECURITY CONSULTING

WHAT KIND OF TASKS SHALL AN ENTITY COMPLETE?

Organisations involved in cyber security monitoring must carry out the following tasks:

- Policies on risk analysis and information system security
- incident handling;
- business continuity, such as backup management and disaster recovery, and crisis management;
- supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;
- security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;
- policies and procedures to assess the effectiveness of cybersecurity risk-management measures;
- basic cyber hygiene practices and cybersecurity training;
- policies and procedures regarding the use of cryptography
- human resources security, access control policies and asset management;
- the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

COMPETENT AUTHORITIES, SANCTIONS & PENALTIES

Each Member State shall designate or establish one or more competent authorities responsible for cybersecurity and for the supervisory tasks, shall monitor the implementation of this Directive at national level, and establish a single point of contact.

When concerned entities do not fulfill the cybersecurity requirements or do not comply with the procedural steps, the competent authority is entitled to:

- issue a warning;
- order the entities concerned to implement the recommendations provided as a result of a security audit within a reasonable deadline;
- prohibit concerned entities from further operation.

Upon unsuccessful measures the authority is further entitled to issue administrative fines, which:

- Can be of a maximum of at least EUR 10 000 000 or of a maximum of at least 2 % of the total worldwide annual turnover in the preceding financial year;
- Can be of a maximum of at least EUR 7 000 000 or of a maximum of at least 1,4 % of the total worldwide annual turnover in the preceding financial year.

HOW CAN AAM CONSULTING LTD. HELP YOU?

Our colleagues bear several decades of experience in implementing IT and Information Security projects in the Central and Eastern European region.

Our qualifications:

- Certified Information Systems Auditor (CISA)
- ISO/IEC 27001 Lead Auditor
- Information and Communication Technology vocational counsel
- Electronic Information Security Manager

- Assessing your current IT security situation (GAP-analysis)
- Preparing your IT security Risk Assessment
- Classification of your IT Systems and stored data
- Establish and review your Information Security Management System (and regulations)
- Providing professional consultation and advice on implementing IT security measures
- Serving as an Infromation Security Officer for your company
- Providing IT Security Awareness materials and Tranings for your employees

AAMs regional team, experienced in risk assessment, risk management, compliance preparation programs, can support group wide NIS2 projects with local consultants in multiple countries including: Hungary, Bulgaria, Slovakia, Slovenia, Croatia, Romania.

AAM CONSULTING

AAM Consulting
Capital Square Offices, 76, Váci út,
1133 Budapest, Hungary
Phone: +36 1 465 2070, +36 1 688 66 88
Web: https://www.aam.hu/
E-mail: aam@aam.hu

AAM Consulting Bulgaria
17, ul. Moskovska,
1000 Sofia, Bulgaria
Phone: +359 878 32 03 04
Web: https://www.aamconsulting.bg/
E-mail: aambulgaria@aam.hu